

ISS News

August 2006

Information Systems Security (ISS)

Internet Use and Copyright Restrictions



Did you know?

Government computer systems and networks are monitored on a regular, on-going basis. As an employee, contractor, or subcontractor you have consented to such monitoring through your use of these systems and networks. Do you also know that you can be held liable to **investigation, prosecution or disciplinary action** based on the inappropriate use of these systems and networks? This issue of our newsletter was designed to help you understand USDA policies on inappropriate use of computer systems, networks and the internet.

Could you be engaging in unauthorized use of the internet and not even realize it?

If you have to ask yourself whether or not you should download software from the internet or if you should access a particular web site, then the rule of thumb is that you probably should NOT do it. USDA computer systems and networks are to be used only for official USDA business.

If you have questions regarding the proper use of the internet, check with your supervisor.

Using Peer to Peer (P2P) Software...

A growing concern within ISS is the increasing number of user's who download and use Peer-to-Peer (P2P) software. P2P software enables the user to download other software, music, graphics or videos, including pornographic materials. This creates security problems as these programs also have the ability to send inbound and outbound traffic to your computer, thus disguising their purpose and allowing others to view and download files from your computer systems. Some prohibited P2P products include: gnutella, LimeWire, SwapNut, KaZaA, Morpheus, AOL Instant Messenger, Yahoo Messenger, Skype and MSN Messenger. Attached is a copy of the Cyber security memo outlining additional examples of PSP software.

P2P software programs allow others to access shared resources on computer systems with similar P2P products, thus making your system vulnerable and insecure.

USDA Policy on Internet Use and Copyright Restrictions

USDA has a long established policy that does not condone or support employee's use of Government computer systems or networks for unauthorized purposes. P2P programs and downloaded software programs have no recognized departmental business need and should not be loaded on workstations or equipment used to conduct USDA Official Business without an approved exception from the Associate CIO for Cyber Security.

Specifically, USDA employees are prohibited from loading P2P software on USDA equipment, downloading illegal material, downloading copyrighted material for personal use, and the distribution of illegally obtained files and software. The "Limited Personal Use Policy" defined in DR 3300-1 cannot be used as a justification for downloading P2P or other programs that perform those functions, downloading or distributing pornographic material or copyright infringement. To read the full policy go to <http://www.ocio.usda.gov/directives/index.html> and open DM 3525-002 "USDA Internet Use and Copyright Restrictions."

What is unauthorized computer & internet usage?

USDA computer systems and networks are to be used only for official USDA business. Unofficial use includes such things as browsing gambling or sexually explicit sites, conducting unofficial business or spending significant time online. Such use is prohibited. Employees are permitted limited personal use of the internet, as indicated in APHIS Directive 3140.3 before or after work, and during designated lunch periods and breaks. Employees may not use government computer equipment to engage in a for-profit personal business.

For additional information:

- **DM 3500 - 3599 - Cyber Security** (Available on the USDA web site, www.usda.gov)
- **Billy Smith**, Acting Information Systems Security Program Manager, 301-734-7604